REMARKS

Applicant respectfully requests reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow. Claims 1, 12 and 25 have been amended. Claims 52-57 have been canceled. Claims 58-63 have been added. Claims 12 and 25 have been amended to change form preference. Claims 58-63 replace Claims 52-57. Claims 1-12, 14-25, 27-51 and 58-63 are now pending in this application. Claims 21-24 and 30-51 are withdrawn.

I. Claim Rejections Under 35 U.S.C. § 101

On page 4 of the Office Action, Claims 1-11, 53, 55, and 57 were rejected under 35 U.S.C. § 101 because the claimed invention is allegedly directed to non-statutory subject matter. Applicants respectfully disagree. In order to further prosecution, Applicants have amended the claims.

Claim 1 has been amended to recite "at a processor." Thus, amended Claim 1 recites a particular machine. Claims 2-11 include the elements of Claim 1.

Claims 53, 55, and 57 have been canceled rendering the rejection moot. New Claims 58, 60 and 62 recite "non-transitory." The use of "non-transitory" is to be understood to remove only propagating transitory signals per se from the claim scope and does not relinquish rights to all standard computer-readable media that are not only propagating transitory signals per se. The meaning of "non-transitory computer-readable medium" should be construed to exclude only those types of transitory computer-readable media which were found in Nuijten to fall outside the scope of patentable subject matter under 35 U.S.C. §101.

Applicants submit that Claims 1-11, 53, 55, and 57 are directed to patentable subject matter under 35 U.S.C. § 101. For at least these reasons, Applicants respectfully request withdrawal of the rejection of Claims 1-11, 53, 55, and 57 under 35 U.S.C. § 101.

II. Claim Rejections Under 35 U.S.C. § 103

On page 5 of the Office Acton, Claims 1-12, 14-20, 25, 27-29, and 52-57 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,748,533 to Wu, et al. (hereafter "Wu") in view of U.S. Patent No. 6,119,932 to Maloney, et al. (hereafter "Maloney"). Applicants respectfully traverse the rejection. Wu and Maloney, alone or in combination, fail to teach or suggest "verifying the bearer's age when ... the second digital data and the third digital data correspond," as recited in Claim 1. New Independent Claims 58 and 59 include similar features. Further, Wu and Maloney, alone or in combination, fail to teach or suggest "determining, based on the first set of information, the person's age or age level in connection with an age-related transaction or event, wherein said act of determining protects the anonymity of the person in possession of the identification document from said multi-purpose electronic processor or entity performing said determining," as recited in Claim 12, or "wherein neither the data corresponding to the second field nor the reduced-bit representation betray the identity of the bearer of the identification document to said multi-purpose electronic processor or an entity performing said act of comparing," as recited in Claim 25. New independent Claims 60-63 include similar features.

Claims 1-11 and 52-53

On page 6 of the Office Acton, the Examiner argues (with underlining added):

> receiving third digital data corresponding to a biometric sample, wherein the biometric sample corresponds to the bearer; and (col. 10, lines 53-67 and col. 11, lines 5-13)
>
> verifying the bearer's age when: i) the first digital data indicates that the bearer is at least as old as a predetermined age (col. 7, lines 20-28), and ii) the second digital data and the third digital data correspond. (col. 5, lines 14-33 and col. 9, lines 1-22)
>
> Wu discloses generating an invisible watermark and embedding an invisible watermark in an official seal increases verifiable authenticity of the article requiring against forgery or any other

> unauthorized modification (col. 12, lines 48-53). Wu discloses one or several invariant features combined can encrypted by hashing or to produce a random pattern using the extracted message and combine the original content and the generated pattern to generate a watermark (col. 8, lines 28-30 and col. 9, lines 43-45). Wu discloses verifying the legitimacy of the article embedded with linked watermarks where watermark is known in the art to protect owner/person of the identification document being identified or copy protected from unauthorized people. In addition, Wu includes encryption or cryptographic link (Wu - col. 2, lines 30-42), where this is also known to protect the owner/person from unauthorized people. As such, Wu's invention protects a person's anonymity. However, Wu did not clearly discuss the first digital data indicates that the bearer is at least as old as a predetermined age.

Applicants respectfully disagree. Wu and Maloney do not whatsoever disclose or suggest "verifying the bearer's age when ... the second digital data and the third digital data correspond," as recited in Claim 1.

Wu discloses "a method of embedding linked watermarks in an article requiring protection against forgery." (Col. 2, lines 3-5, See also Cols. 2-5; Underlining added). In particular, column 10, lines 53-67, cited by the Examiner, disclose:

> FIG. 5 is a flow diagram illustrating an exemplary process of extracting invariant biometrics feature, which can be practiced with the embodiments of the invention. Processing commences with the input of biometrics data, such as a person's facial image 500 or fingerprint, for example. Other types of biometrics data may be practiced with the embodiments of the invention without departing from the scope and spirit of the invention. In step 504, the biometrics data (e.g. facial image 500 or fingerprint 502) is electronically scanned and digitized. Optionally, step 506 may be carried out if necessary to pre-process the digital data. This can involve filtering, or enhancing the data content, for example. Other conventional techniques of processing digital data can be practiced without departing from the scope and spirit of the invention.

However, column 11, lines 1-18, also describing FIG. 5, disclose (with underlining and emphasis added):

> In step 508, the digital data (i.e. image) is normalized in both space and intensity based on predefined rules and landmarks. In step 510, one or more features are extracted from the normalized data. In step 512, recognition processing of the extracted features is carried out to identify invariant features. Any of a number of recognition methods can be practiced. For some recognition methods, the recognition base 514 may be required as input to the recognition engine in step 512. For example, in a facial recognition system, an eigenface technique can be practiced. The eigenfaces (recognition base) are previously produced by training facial samples. The invariant features can be determined by computing a projection of an input facial image onto the eigenfaces. As this is optional dependent upon the recognition method used, it is depicted using dashed lines. Finally, in step 512, the invariant biometrics features 516 are obtained using the recognition engine. The invariant features 516 can be output to the watermark **generator.** Normally, these features 516 have a size of a few hundred bytes.

Further, the bottom of FIG. 5 indicates that the output of the flow diagram goes "[t]o [a] watermark generator." Thus, Wu merely discloses extracting invariant biometrics features in order to generate a watermark.

In contrast, Claim 1 recites "verifying the bearer's age when ... the second digital data [corresponding to a biometric indictor] and the third digital data [corresponding to a biometric sample, wherein the biometric sample corresponds to the bearer] correspond," as recited in Claim 1. Extracting invariant biometrics features in order to generate a watermark as in Wu is not equivalent to "verifying the bearer's age when ... the second digital data and the third digital data correspond," as recited in Claim 1.

Maloney discloses an "identification verification apparatus []. The apparatus is of the type that includes a camera for capturing an image of a user and a storage device that stores the captured image." (Col. 1, lines 47-51; Underlining added). In particular, Maloney discloses:

> The storage device 22 is preferably a video tape recorder, such as Sanyo Model No. SRT 500 or SRT 600, but may alternatively be any electronic or magnetic storage medium. The camera 20 may be a CCD low light level camera or any other suitable camera. In

> addition, the camera 20 is preferably equipped with a wide angle lens. Many suitable cameras and lenses for this application are commercially available. For example, the camera 20 may be a Konica/Chugai Model No. FC62B (Black & White, 1/3", CCD) equipped with a Computer/Chugai 4 MM lens, Model No. TO412FICS. Likewise, numerous commercially available monitors are suitable for this application, such as the Ultrak Model Nos. KM9 and KM12.

(Col. 2, lines 53-65; Underlining added). Further, Maloney discloses:

> The identification verification apparatus shown in FIGS. 1A and 1B operates as follows when used in conjunction with an operator. When a customer or patron approaches the operator of the apparatus, the camera 20 captures an image of the customer. The image is transferred in electronic form from the camera 20, through the video interface 32, to the storage device 22. ...In addition, the storage device 22 may superimpose time and date information on the recorded image.
>
> The customer then presents an identification card or the like to the operator, who uses the data detection device 24 to read data from the identification card. The data is decoded by the decoder 30 and then transmitted to the microprocessor 26 and the video interface 32. At the microprocessor 26, the data is preferably formatted and stored as a database entry. A monitor (not shown) may be connected to the microprocessor and located within view of the operator to provide the operator with instructions, such as whether the data was properly read from the identification card, or information derived from the data.

(Col. 4, lines 22-43; Underlining added). Thus, Maloney merely discloses a device for recording images of a customer who also presents identification, which can be scanned as described in column 5, lines 26-67. Maloney does not whatsoever use the stored image for a comparison.

In contrast, Claim 1 recites "verifying the bearer's age when ... the second digital data [corresponding to a biometric indictor] and the third digital data [corresponding to a biometric sample, wherein the biometric sample corresponds to the bearer] correspond," as recited in Claim

1. Storing the image of a customer as in Maloney is not equivalent to "verifying the bearer's age when ... the second digital data and the third digital data correspond," as recited in Claim 1.

An obviousness rejection cannot be properly maintained if the references cited do not disclose each and every element of the claims. For at least these reasons, amended Claim 1 is patentable over Wu and Maloney, alone or in combination. Claims 2-11 depend from Claim 1. Claims 52 and 53 are canceled. For at least these reasons, Applicant respectfully requests withdrawal of the rejection of Claims 1-11 and 52-53 under 35 U.S.C. § 103. New Claims 58 and 59 are patentable over Wu and Maloney for at least the same reasons as Claim 1.

Claims 12, 14-20, 25, 27-29, and 54-57

The Examiner does not present arguments regarding the feature "determining, based on the first set of information, the person's age or age level in connection with an age-related transaction or event, wherein said act of determining protects the anonymity of the person in possession of the identification document from said multi-purpose electronic processor or entity performing said determining," as recited in Claim 12. However, with regard to Claim 25, on page 6 of the Office Acton, the Examiner argues (with underlining added):

> wherein neither the data corresponding to the second field nor the reduced-bit representation, betray the identity of the bearer of the identification document to said multi-purpose electronic processor or an entity performing said act of comparing. (col.12, lines 1-9 and 44-67 and col.13, lines 15-27).

Applicants respectfully disagree. Wu and Maloney do not whatsoever disclose or suggest "determining, based on the first set of information, the person's age or age level in connection with an age-related transaction or event, wherein said act of determining protects the anonymity of the person in possession of the identification document from said multi-purpose electronic processor or entity performing said determining," as recited in Claim 12, or "wherein neither the data corresponding to the second field nor the reduced-bit representation betray the identity of the

bearer of the identification document to said multi-purpose electronic processor or an entity performing said act of comparing," as recited in Claim 25.

Wu discloses "a method of embedding linked watermarks in an article requiring protection against forgery." (Col. 2, lines 3-5, See also Cols. 2-5; Underlining added). In particular, column 12, lines 1-9 and 44-67, cited by the Examiner, disclose (with underlining and emphasis added):

> In step 618, the adjusted watermark is printed, output or otherwise embedded in the assigned portion or working area. In this connection, FIGS. 1 and 2 illustrate the relationships between the generation of watermarks using data from one area and the embedding of the watermark in another area. The encryption used in the first embodiment is used not only for the purpose of concealment but also for the purpose of verification of the article or product 100. As biometric features and recognition/extraction techniques are known, those skilled in the art will appreciate that the selection and encryption of the extracted biometrics information 600 and other appended messages 602 are helpful to guarantee the security of watermark generators and the whole system. Meanwhile, the authentication is carried out using the encrypted selected message and extracted watermark. **This is like verifying a digital signature.**
>
> ...
>
> FIG. 7 is a block diagram depicting an article 700 containing security information according to the second embodiment. The depicted exemplary article 700 is a passport. However, the article can be any of numerous products requiring protection against forgery, including a credit card, a bank note, a lottery ticket, a legal document, a driver's license, a birth certificate, etc. Embedding an invisible watermark in an official seal increases the verifiable authenticity of the article 700 requiring protection against forgery or any other unauthorized modification.

Further, column 13, lines 15-27, cited by the Examiner, disclose (with underlining added):

> ... By embedding a watermark 714 within an official seal 712, it can be ensured that the document has been properly averred to or authorized and that its contents have not been changed and only contain the information that the authorizing authority considered. In this manner, a certifiable official seal is provided.
>
> Alternatively, a watermark can be embedded in the seal containing information about the authority alone or in combination with information described above. The invisible watermark authenticates and protects the owner of the seal that is applied. Only the authority has access to an unwatermarked copy of the seal. All other copies of the seal available to the public are embedded with an invisible watermark.

Thus, Wu merely discloses that a watermark to protect against forgeries. Nothing in Wu discloses or suggests that anonymity is preserved.

In contrast, Claim 12 recites suggest "determining, based on the first set of information, the person's age or age level in connection with an age-related transaction or event, wherein said **act of determining** protects the anonymity of the person in possession of the identification document **from** said multi-purpose electronic processor or entity performing said determining," and Claim 25 recites "wherein neither the data corresponding to the second field nor the reduced-bit representation betray the identity of the bearer of the identification document **to** said multi-purpose electronic processor or an entity performing said act of comparing," as recited in Claim 25. Merely verifying the a document is not a forgery as in Wu is not equivalent to where "**act of determining** protects the anonymity of the person ... **from** said multi-purpose electronic processor or entity performing said determining," as in Claim 12 or where "the data [does not] betray the identity of the bearer of the identification document **to** said multi-purpose electronic processor or an entity performing said act of comparing," as in Claim 25.

Maloney discloses an "identification verification apparatus." (Col. 1, lines 47-51). In particular, in column 5, lines 26-67, Maloney discloses (with underlining added):

> At step 210, the identification card is scanned and the date of birth, for example, is captured from the identification card. During step

> 210, the scanned data is read from the identification card and written to the file that was opened at step 190. ...
>
> At step 230, the date of birth information is located within the scanned data. Then, at step 240, the date of birth information from the identification card is compared to the legal access date calculated at step 170. If the date of birth information indicated that the customer is of an appropriate age, then the program proceeds to step 250, where the scanned information is formatted and stored as a database entry. If the date of birth information indicated that the customer is not of an appropriate age, then the program may optionally proceed to format and store the scanned information in a separate database. A program listing demonstrating how the scanned information is formatted and stored is attached hereto in Appendix B. Preferably, a separate database entry is created for each customer. From step 250, the program returns to step 200 and is ready to scan the next identification card. If, on the other hand, the date of birth information indicates that the customer is not of an appropriate age at step 240, the program proceeds to step 260 where an indicator is provided to the operator. From step 260, the program returns to step 200.

Thus, Maloney merely discloses that date of birth information is located and, for each customer, stored in a database. Further, as discussed above, Maloney stores an image of the customer. Nothing in Maloney discloses or suggests that anonymity is preserved.

In contrast, Claim 12 recites suggest "determining, based on the first set of information, the person's age or age level in connection with an age-related transaction or event, wherein said **act of determining** protects the anonymity of the person in possession of the identification document **from** said multi-purpose electronic processor or entity performing said determining," and Claim 25 recites "wherein neither the data corresponding to the second field nor the reduced-bit representation betray the identity of the bearer of the identification document **to** said multi-purpose electronic processor or an entity performing said act of comparing," as recited in Claim 25. Storing the birth date of each customer in a database along with an image of the customer as in Maloney is not equivalent to where "**act of determining** protects the anonymity of the person ... **from** said multi-purpose electronic processor or entity performing said determining," as in

Claim 12 or where "the data [does not] betray the identity of the bearer of the identification document to said multi-purpose electronic processor or an entity performing said act of comparing," as in Claim 25.

An obviousness rejection cannot be properly maintained if the references cited do not disclose each and every element of the claims. For at least these reasons, Claims 12 and 25 are patentable over Wu and Maloney, alone or in combination. Claims 14-20, 25, and 27-29 depend from one of Claims 12 and 25. Claims 54-57 are canceled. For at least these reasons, Applicant respectfully requests withdrawal of the rejection of Claims 14-20, 25, 27-29, and 52-57 under 35 U.S.C. § 103. New Claims 60-63 are patentable over Wu and Maloney for at least the same reasons as Claim 12 and 25.

* * *

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by the credit card payment instructions in EFS-Web being incorrect or absent, resulting in a rejected or incorrect credit card transaction, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date March 9, 2011

By */Eric N. Huston/*

FOLEY & LARDNER LLP
Customer Number: 99103
Telephone: (608) 258-4205
Facsimile: (608) 258-4258

Eric N. Huston
Attorney for Applicant
Registration No. 65,684